Response to FCC Notice of Proposed Rulemaking for Digital Broadcast Copy Protection

MB Docket No. 02- 230

December 5, 2002

Submitted by:

Digimarc Corporation
19801 72nd Ave., Suite 100
Tualatin, OR 97062 USA

Contact: Reed Stager
VP, Global Licensing
Phone: 503-495-4562
E-mail: rstager@digimarc.com

Macrovision Corporation
2830 De La Cruz Boulevard
Santa Clara, CA 95050 USA

Contact: Bill Krepick
President and CEO
Phone: 408-562-8464
E-mail: BKrepick@macrovision.com

Table of Contents

FCC Response by Digimarc and Macrovision: Mandate for Digital Broadcast Copy Protection Rules 3
1 Executive Summary 3
2 Introduction 3
3 Problem and Complete Solution 4
3.1 Broadcast Flag is a Partial Solution 4
3.2 Security Flaw with the Broadcast Flag is the Analog Hole 4
3.3 The Analog Hole is Huge and Forever 6
3.4 Supporting Experiences from the Audio Market 6
3.5 Digital Watermarks Plug the Analog Hole 7
3.6 Broadcast Watermark replaces Broadcast Flag 9
3.7 Multiple Architectures enabled by Broadcast Watermark 9
3.8 Cost of System Implementation 10
3.9 Status of Digital Watermark Technology 10
3.10 Benefits of Digital Watermark Technology 11
4 Answers to Questions 11
4.1 Digital Broadcast Copy Protection Questions 11
4.2 Reception of the Digital Broadcast Signal Questions 12
4.3 Impact on Consumers based Questions 13
5 Conclusion 14

FCC Response by Digimarc and Macrovision: Mandate for Digital Broadcast Copy Protection Rules

1 Executive Summary

Digimarc and Macrovision believe that the Notice of Proposed Rulemaking (NPRM) based upon the Broadcast Flag does not represent a technically sufficient solution to protect broadcast content from unauthorized distribution, and, thus, does not represent an activity that is worth the significant implementation costs to industry and consumers that are involved. The Broadcast Flag leaves analog outputs and rendered content unprotected. This deficiency has become generally referred to as the "Analog Hole". Entertainment, as rendered content, must always be delivered in analog format, regardless whether it is distributed in digital or analog format, since the human eyes and ears are analog. Analog outputs will be available for the foreseeable future since it is unreasonable to believe that most of the 105M homes with analog TVs and 92M homes with analog VCRs will be converted by 2006. The persistence of analog outputs is supported from experiences in the audio market, where digital only copy protection failed and left audio CDs "completely unprotected," as stated by Record Labels.

With only the Broadcast Flag, rendered content and the broadcasts streamed from analog outputs can easily be digitally recorded and redistributed, thus enabling an average consumer without any special equipment to bypass the Broadcast Flag.

Broadcast Watermark technology is a better solution than the Broadcast Flag as it is viable for both analog and digital video content protection. Like the Broadcast Flag, the Broadcast Watermark can also signal the *no redistribution* state, but the watermark is the only technology that survives the Analog Hole, thus, protecting content that re-enters the digital environment via the Analog Hole. As such, Digimarc and Macrovision believe that it is appropriate for the NPRM to set a course to standardize a Broadcast Watermark rather than a Broadcast Flag.

2 Introduction

Based upon the questions asked by the FCC in a press release from August 8, 2002 and in MB Docket No. 02-230 entitled "NOTICE OF PROPOSED RULEMAKING" released August 9, 2002, Digimarc and Macrovision are providing the answers in this document.

This document answers these questions in the next two sections. Section 3 provides a general overview of the situation. Section 4 includes answers to each question posed in the FCC announcement.

3 Problem and Complete Solution

This section demonstrates the security flaw with a Broadcast Flag solution, and describes how a complete security solution, where the Analog Hole is secured, is provided with a Broadcast Watermark.

The Broadcast Watermark is a digital watermark that can carry the *no redistribution* state like the Broadcast Flag, but the Broadcast Watermark survives digital processing and format conversion, as well as conversion to analog, analog processing, and the conversion back to digital.

3.1 Broadcast Flag is a Partial Solution

The focus of Broadcast Protection Discussion Group (BPDG), a subgroup of the DVD Copy Protection Technical Working Group (CPTWG), was the prevention of unauthorized redistribution of unencrypted digital terrestrial broadcast content, as indicated in the BPDG's charter. Compliant devices, upon detecting content marked with a Broadcast Flag are required to protect its digital outputs. This means that the broadcast content will not remain self-protected but instead protection becomes dependent on a maze of equipment requirements which must be correctly transferred from one product to another, and all protection is lost in case of analog connections. Using the Broadcast Flag to mark the content only provides a trivial level of security. Consumers that don't have much technical competence can easily use the analog outputs and off the shelf technology to digitize and redistribute the content (a.k.a. the Analog Hole).

3.2 Security Flaw with the Broadcast Flag is the Analog Hole

The Analog Hole is an issue of much discussion. The Analog Hole has been defined by Richard Parsons, CEO of AOL Time Warner at the Senate Judiciary Hearing of March 14th, 2002 as:

> "Video content, even when delivered digitally in a protected manner, must be converted to an unprotected analog format to be viewed on the millions of analog television sets in consumer homes. Once content is "in the clear" in analog form, it can be converted back into digital format which can then be subject to widespread unauthorized copying and redistribution, including over the Internet. This problem applies to all delivery means for audiovisual content, from DVDs to pay per view, to over the air broadcasts."

Thus, the security flaw with the Broadcast Flag is:

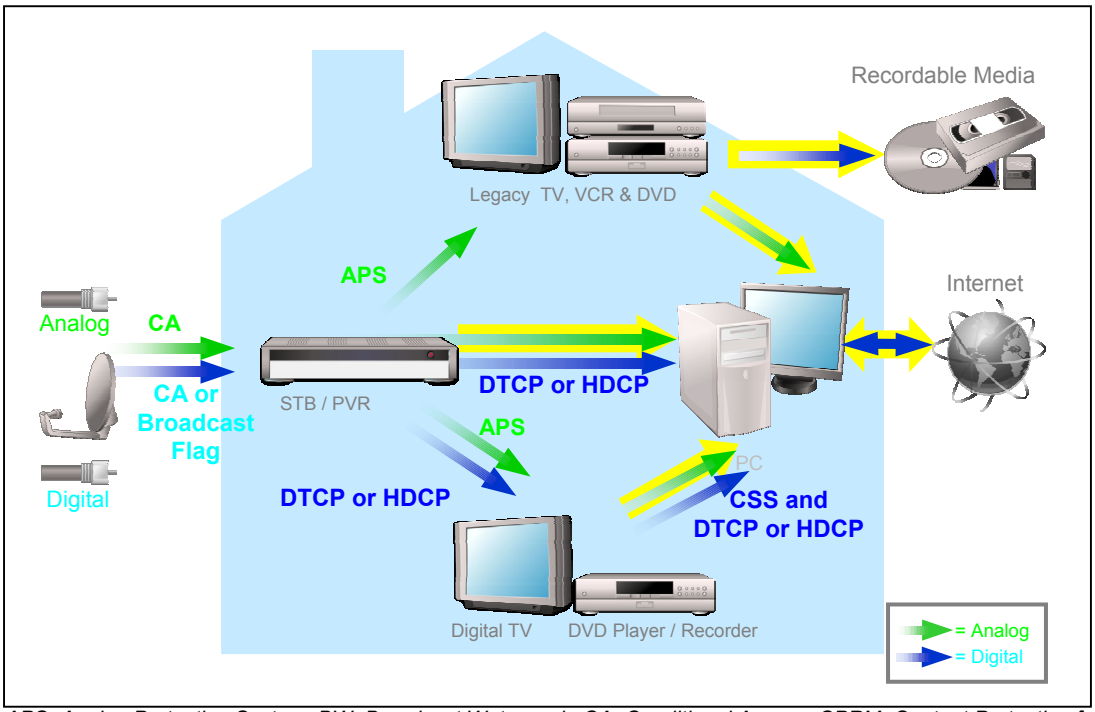
- Analog outputs of digital broadcast receiving devices, such as a set-top box (STB)

The analog outputs are as good as the digital HD outputs for illegitimate redistribution. In practice, both digital and analog captured video, recompressed for the Internet will look identical. Many DVD-recorders when offered a digital Video stream in a slightly different format than the one used on the disc, will render digital formats by converting via analog.

Another open issue includes backwards compatibility during the transition period, defined as the period during which analog broadcasts are converted to digital broadcasts and TVs begin receiving standard-definition (SD) and high-definition (HD) digital input. Currently, the vast majority of Digital TVs employ a STB ATSC receiver with analog HD connections to a CRT monitor. Similarly, Open Cable STBs provide for analog HD connections to the CRT monitor. These analog HD connections are not currently provided with any form of protection, and would not be protected by the Broadcast Flag.

The Broadcast Flag does not protect these HD analog outputs and other outputs since the Flag is a digital header technology that is lost with conversions like conversions to analog. This is because the Broadcast Flag does not protect the content but the channel. These HD analog outputs cannot be scrambled because then all of the existing HDTVs would not work.

An exemplar system with only the Broadcast Flag is shown in the diagram below, where unprotected content can easily be copied and sent to the Internet or recordable media from the analog or legacy digital channels (as highlighted in yellow).



APS=Analog Protection System, BW=Broadcast Watermark, CA=Conditional Access, CPRM=Content Protection for Recordable Media, CSS=Content Scrambling System, DTCP=Digital Transmission Content Protection, and HDCP=High-bandwidth Digital Content Protection.

3.3 The Analog Hole is Huge and Forever

The Analog Hole will exist forever, as entertainment distribution and rendering technology continue to improve the efficiency and effectiveness of networks and receivers. This is immutably true because the ultimate consumers – human beings – will always consume the video and audio content with their ANALOG eyes and ANALOG ears.

There have been suggestions to mitigate the effect of the Analog Hole by banning analog outputs. Besides being a futile effort, for the reasons stated above, such a quixotic quest would be devastatingly costly for consumers. The analog receiver market is huge. The normal useful life of these products would span a decade or more, absent forced obsolescence. A forced early sunset of these products would cost consumers hundreds of millions of dollars of lost utility. TVs and related products are often very large purchases within family budgets. This would create an unnecessary hardship for consumers in the 105 million households with 273 million analog TV sets or the 92 million households with analog VCR's in the United States.

And remembering that TVs and VCRs have a useful life of at least 10 years, consumers would react very negatively to initiatives that artificially limit the usefulness of their TV's or forces them to buy new ones.

Even if proposed legislation that

- Requires digital tuners in all TVs by 2007
- Eliminates analog broadcasts by January 2006
- Removes analog outputs of TVs by July 2005

was enacted, it would **not** eliminate the Analog Hole since all digital receiving devices, such as STBs, will be required to support this massive number of analog TVs and VCRs. It would not be in the best interest of the public to require or a consumer electronics company to produce a STB, PVR, and/or DVD device that does not support these 273 Million analog TV sets.

As such, the analog outputs will exists for decades, and the Analog Hole will never go away.

3.4 Supporting Experiences from the Audio Market

Similar experiences in the audio market reinforce the fact that analog connections will remain and digital only based solutions, like the Broadcast Flag, will fail.

In the early 1990's digital-only protection using a serial copy management system was the way audio CD-protection had been agreed on between the content and hardware industries. It was expected that analog connections would disappear, but that proved entirely incorrect. Despite two decades of digital audio (CD), digital recorders, and delivery of digital audio via Internet delivery, digital connections did not grow in usage.

In the end, serious technical investments and years of legislative efforts on digital only solutions have failed, exemplified by the continued claim by Music Industries that CD's are "entirely unprotected".

3.5 Digital Watermarks Plug the Analog Hole

The Analog Hole must be secured to provide an effective solution for protecting digital broadcast content. Otherwise, pirates will take the path of least resistance and use the security flaw left by the Broadcast Flag to easily copy the content from a quality analog output, re-digitize it, and redistribute it. It is so easy that the average consumer can bypass the Broadcast Flag without any special equipment, thus rendering the digital protection ineffective.

Digital Watermarks reside in the broadcast content rather than the content channel and therewith protect independent of applied technology, analog or digital. Digital watermarks have been identified to help secure both the Analog Hole and the digital domain, as noted in the following recent quotes from leaders in the technology, motion picture, and government sectors:

> "Watermarks may provide a means to ensure that protection rules survive as content transitions analog outputs."
>
> Dr. Craig R. Barrett, President and CEO, Intel Corp. Senate Judiciary Hearing, March 14th, 2002.

> "We are developing a plan to plug the "Analog Hole" that includes harnessing watermarking technology that would prevent such conversions from being used to avoid content protection obligations"
>
> Peter Chernin, President and COO, News Corporation
> Senate Commerce, Science and Transportation Committee Hearing, February 28th, 2002.

> "One way to plug the Analog Hole is through the use of watermarks…. some government action will be needed to require appropriate detection of and response to the watermark."
>
> Richard Parsons, CEO, AOL Time Warner, Inc.,
> Senate Judiciary Hearing, March 14th, 2002

> "The most promising technical solution for this so-called "Analog Hole" appears to be watermarking copy control technology…"
>
> The Honorable Patrick Leahy, U.S. Senator, Vermont,
> Chairman of Senate Judiciary Committee,
> Senate Judiciary Hearing, March 14th, 2002

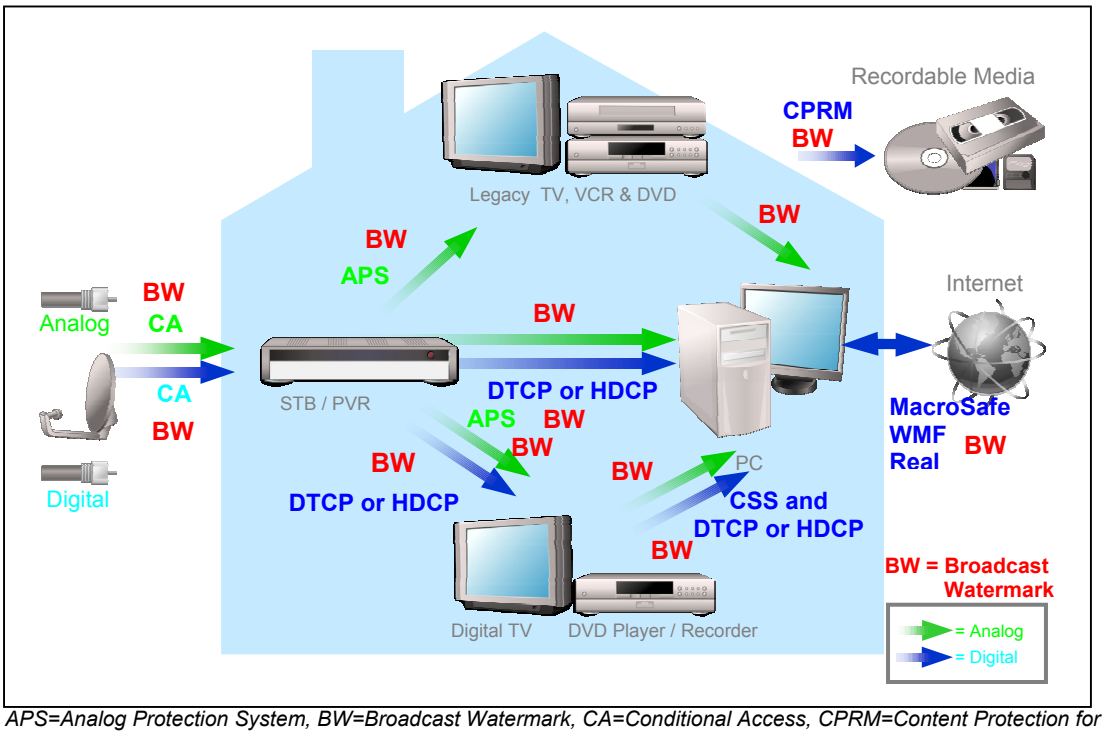
> "If we can get to the moon or get to Mars… why can't we put a little watermark on our content?"
>
> Michael Eisner, CEO, Walt Disney
> Fortune, May 27, 2002

The Broadcast Watermark was originally identified as an alternative in the November 28th presentation by 5C to the CPTWG and discussed during the BPDG meetings, without any consensus

Digimarc and Macrovision believe that in order to comprehensively prevent digital television content from unauthorized redistribution, the Analog Hole must be secured and that a Broadcast Watermark must be used.

In addition to providing protection against the Analog Hole, a Broadcast Watermark enables content to work with legacy devices and remain protected. Specifically, the Broadcast Watermark remains with the content in legacy devices and network connections, and enables the content to be protected when entering a compliant device. We refer for example to tests performed on the watermark system for DVD in which multiple cascaded recordings on VCR did not remove the watermark.

An exemplar complete system, where the content is always labeled on the Internet or within recordable media, is shown in the diagram below. Note that the Broadcast Flag would have only existed between the digital broadcast and receiving digital broadcast equipment, such as STB/PVR combo, whereas the Broadcast Watermark survives all connections, even analog, to always maintain the *no redistribution* state within the content.



APS=Analog Protection System, BW=Broadcast Watermark, CA=Conditional Access, CPRM=Content Protection for Recordable Media, CSS=Content Scrambling System, DTCP=Digital Transmission Content Protection, HDCP=High-bandwidth Digital Content Protection, MacroSafe=Macrovison's DRM, Real=Real Network's DRM, and WMF=Microsoft Windows Media File DRM.

3.6 Broadcast Watermark replaces Broadcast Flag

In order to truly protect the content and eliminate the inappropriate redistribution and piracy of broadcast content, it is important to use available technology. This should include a Broadcast Watermark, which can help protect both digital and analog content, including analog content that has been digitized for redistribution or playback.

The Broadcast Watermark provides the following critical security features:

- Protecting the analog outputs of digital broadcast receiving devices (a.k.a. plugging the Analog Hole)
- Backwards compatibility with legacy equipment during the transition period
- Additional layer signaling the *no redistribution* state if/when the output encryption is broken such that compliant devices respect the *no redistribution* state

The Broadcast Watermark is compatible with encryption. Once inserted into content it will remain in the content and, thus, reflect much more a notion of self protected content. Watermarks function through all digital and analog connections and even when the encryption is compromised, the Broadcast Watermark remains. The Broadcast Watermark can force the reassertion of usage rights when content transitions into a device with a watermark detector (i.e. a compliant device).

In summary, as discussed above, the Broadcast Watermark plugs the Analog Hole, can be used in both the analog and digital domain, and is backwards compatible with legacy equipment. This enables protecting analog outputs for legacy TVs, as well as being backwards compatible with legacy equipment, which means that no consumer will be left with unusable legacy equipment.

3.7 Multiple Architectures enabled by Broadcast Watermark

A Broadcast Watermark could be used by a variety of implementations that protect content downstream, including both the reference architecture proposed by the 5C and one of the Philips' proposals known as "the flag preserving architecture."

In the reference 5C architecture, a Broadcast Watermark can be used to signal the digital broadcast receiver to encrypt the outputs. In addition, the Broadcast Watermark can survive analog outputs and conversion back to digital, such that other digital broadcast devices can detect a Broadcast Watermark and act appropriately, according to a standardized set of usage rules, while enabling legacy devices to function properly.

In alternative architectures, such as the initial Philips proposal of flag preserving architecture (which we do not describe here, but is available from the BPDG archives), a Broadcast Watermark can work in the analog and digital domain. In fact, a Broadcast Watermark is more robust than the Broadcast Flag because, as being part of the content, it is inherently preserved without specialized hardware.

3.7.1 Synergies between Broadcast and DVD consensus Watermark

If the Broadcast Watermark is synergistic with the DVD consensus watermark, compliant DVD recorders and PC recorders can be made to respect the *no distribution* state. The watermarks can be synergistic by simply using the DVD consensus watermark with a no redistribution state along with the copy never, copy one generation, copy no more, and copy freely states as currently defined by the DVD CPTWG.

This protection can be limited to analog channels, but can easily include digital channels, since the same watermark detector can be used to detect a watermark on an analog or digital channel. Given the availability of DVD copy protection watermark technology there is no reason not to proceed with the utmost speed in defining and implementing a Broadcast Watermark.

3.7.2 Architectures that enable Consumer Fair Use Expectations

Broadcast Watermarks can be used in an alternative architecture that enables consumer fair use expectations. Once these are defined, the architecture can be enabled with a Broadcast Watermark. For example, with DVD copy protection, the consensus watermark enables copy-once capabilities.

3.8 Cost of System Implementation

The cost of implementation for a Broadcast Watermark and a Broadcast Flag solution are substantially similar. In either case, the cost of the detector is minimal in relationship to implementing the complete system. The complete system includes integrating the inserter/embedder into the broadcast workflow, integrating the detector into the digital broadcast receivers, and protecting the content.

In fact, the Broadcast Watermark system has an advantage over the Broadcast Flag since the Broadcast Watermark, once applied to the source video, survives standard digital and analog processing. As such, the Broadcast Watermark will not be lost or degraded during the broadcast process, whereas the Broadcast Flag may require components to be updated at the various uplink and downlink transmission points for its survival (similarly as required with analog equipment for VBI-based ATVEF triggers). In addition, the Broadcast Watermark can be embedded at the broadcast head end or anywhere else in the broadcast process, and remain with the content for its lifetime without updating any legacy broadcast or receiving equipment.

3.9 Status of Digital Watermark Technology

Digital watermark technology that can be used for standard definition (SD) broadcasts and that survives the analog output and re-digitization of quality content, is mature and ready for market. The technology has matured over these last five years of CPTWG testing with the benefit of tens of millions of dollars of investment. It has gone through extensive testing during DVD CPTWG process. This process included passing Golden eye tests and extensive robustness testing.

Digital watermarking is being used in a variety of counterfeit and piracy deterrence solutions, and digital watermarks are present in billions of objects with millions of detectors deployed. Digital watermarking is currently deployed as an effective security feature in printed and digital content. Digimarc is under contract to a consortium of the world's leading central banks to deter PC-based counterfeiting of currency. Television and radio broadcasts are being monitored via watermarking to audit syndication royalties and advertising runs, and for market research. Digital watermarking has been adopted by music labels to track unauthorized distribution of pre-release music.

The digital watermark implementation proposed to CPTWG is extendable to high definition (HD) broadcasts, and can be demonstrated when the market defines requirements for such technology. In addition, digital video watermark technology can be implemented to survive camcorder recording and high-compression.

3.10 Benefits of Digital Watermark Technology

When designing a security system, the constraints are the balance between the cost of implementation, cost of breaking the system, losses based upon the breaks, how it fits into a complete and layered security system, how consumers right to use their legacy equipment are protected, and ease of use of the technology for a legitimate consumer. A Broadcast Watermark is superior not only in addressing these challenges, legacy issues, and fair use, but also in its ability to identify the content and enable enhanced usage models.

For example, this enhanced Broadcast Watermark can identify the content and enable the user to bookmark, access and purchase related information and content. It can even update errors in Electronic Program Guides (EPG). These enhancements are enabled for analog and digital content.

As such, this security technology can provide a more valuable consumer experience and also increase revenues for content owners and broadcasters, thus helping pay for the infrastructure.

4 Answers to Questions

This section includes answers to each of the FCC proposed questions, according to the three groups of questions defined in the FCC press release of August 8, 2002. The sub-sections below include every question from the press release copied verbatim.

4.1 Digital Broadcast Copy Protection Questions

4.1.1 Is the Broadcast Flag the appropriate technological model to be used?

The Broadcast Flag technology is not technically sufficient to be implemented. A Broadcast Watermark technology provides a more robust and complete solution since it plugs the Analog Hole. As fully described in the section 3, the Broadcast Watermark is

part of the content and robust to transformation, including conversion to analog. This quality enables complete security of digital broadcast content, including plugging the Analog Hole, as well as enabling alternative security architectures that have consumer usage benefits. These benefits include preserving the usability of legacy equipment, as well as enabling enhanced content usage.

4.1.2 Is a government mandate requiring broadcasters and content providers to embed the Broadcast Flag (or other content control mark) within digital broadcast programming necessary?

While the preference has been to allow industry to address this issue, it has become increasingly evident that the industry cannot identify an effective solution. To be effective, the mandate should enable the broadcaster and content provider to embed a Broadcast Watermark that protects the digital broadcasts from re-distribution.

4.2 Reception of the Digital Broadcast Signal Questions

4.2.1 Should the FCC mandate that consumer electronics devices recognize and give effect to the Broadcast Flag (or other content control mark)?

The preference has been to allow the industry to voluntarily select and implement effective technology to protect the content. Given the failure of industry to identify and select an effective technology, it is important that the FCC mandate CE devices to detect a Broadcast Watermark.

4.2.2 What is the appropriate point in a consumer electronics device at which digital broadcast copy protection should begin?

Digital watermarking enables a variety of implementations to support policy and optimize for performance and low cost within consumer devices. The expertise of CE manufactures, broadcasters, and content owners should be used to determine the optimal location of detection of a Broadcast Watermark.

4.2.3 Would a digital broadcast copy protection system be effective in protecting digital broadcast content from improper redistribution?

Yes, a digital broadcast copy protection system based upon a Broadcast Watermark will help keep honest people honest. This means that even if it is broken in the future, it will still be effective since a widespread hack cannot easily be distributed due to the Digital Millennium Copyright Act (DMCA).

As discussed in detail in section 3, if the Broadcast Flag is used, anyone can easily digitize the analog output of the digital broadcast receiver, compress the video, and redistribute on the Internet. This section also demonstrated that the analog output of the digital broadcast receiver will exist for decades due to the existence of hundreds of millions of analog devices, mainly TVs and VCRs, which has also proven to be true in the audio market.

In addition, if the complete security architecture is rushed, it may not enable consumers to easily use and enable fair use for digital broadcasts, and, thus, slow adoption for digital broadcasts. As such, the security architecture of how to respond to marked content needs further defining for this initiative to be successful, as described in section 3.8.

4.2.4 Would digital broadcast copy protection work for digital broadcast stations carried on cable or direct broadcast satellite systems? How?

A Broadcast Watermark can survive any type of broadcast, including digital cable, satellite, and even analog cable and satellite broadcasts. The Broadcast Watermark can be synergistic with a DVD consensus watermark and protect analog outputs of digital cable and satellite from being recorded and played on compliant DVD recorders and players, while enabling legacy DVD recorders to function properly. A Broadcast Watermark, when used in conjunction with a DVD recorder can even enable "copy once" functionality, thus enabling consumer fair use expectations. All that is required is for the Broadcast Watermark to be embedded and consumer equipment related to digital broadcasts to detect the Broadcast Watermark and respect the standardized usage rules.

4.2.5 Should the FCC mandate the use of specific copy protection technologies (such as DTCP/5C or HDCP) in consumer electronics devices that are designed to respond to the Broadcast Flag? And, if so, how would a particular technology receive approval for use and who would be the appropriate entity to make that decision?

The industry should select effective copy protection technologies in an open and fair manner that ensures that the efforts of some powerful companies that do not own relevant technology are not allowed to block the utilization of the best technology and/or force adoption of ineffective technologies that they do own.

4.3 Impact on Consumers based Questions

4.3.1 Will requirements to protect digital outputs interfere with the ability to send DTV content across secure digital networks?

A Broadcast Watermark will survive secure and unprotected digital and analog outputs without any alteration required to the secure digital network. In addition, when a Broadcast Watermark is used in a flag preservation system as opposed to encrypting all digital outputs, the robustness of the Broadcast Watermark enables secure digital networks to function properly, as well as compliant digital devices can detect the Broadcast Watermark at either end of the network and act appropriately.

4.3.2 What is the impact of digital broadcast copy protection mechanisms on existing and future electronic equipment?

A Broadcast Watermark will survive with legacy and future electronic equipment, without any changes to the broadcast infrastructure. The Broadcast Watermark will

allow existing equipment to play content, while future equipment with a detector (i.e. compliant) can act appropriately based upon the standardized usage rules.

Encrypting digital outputs based upon a Broadcast Flag will not allow legacy technology, such as existing digital DVD recorders, DTVs and STBs, to function with the encrypted output.

4.3.3 Will digital broadcast copy protection have an effect on the development of new consumer technologies?

If a Broadcast Flag solution that requires every digital output to be encrypted is adopted, the system may have very limited ability to expand. The system may not be able to handle new equipment, such as that based upon 802.11 (i.e. WiFi) which shares transmission protocols TCP/IP with the Internet. In addition, the system may not be able to handle new business models since the encryption is based upon equipment connections and not a compliant home domain model. However, with a Broadcast Watermark, the digital outputs don't need to be encrypted if the attached devices are authenticated (a.k.a. flag preservation), and the system can be secured with such a license.

5 Conclusion

The Analog Hole must be addressed in crafting an effective means to prevent unauthorized redistribution of unencrypted digital broadcasts. Since the presence of the Analog Hole renders the protection provided by the Broadcast Flag essentially ineffective, the problem must be addressed with implementation of the Broadcast Watermark. No alternative technologies have been identified to effectively resolve the problem.

A Broadcast Watermark can protect the analog output of digital broadcast receivers, is backwards compatible and preserved with legacy DTVs and DVD players, can enable consumer fair use expectations, and provides an additional layer of protection synergistic with digital encryption. The advantages of a Broadcast Watermark solution are based upon the fact that the digital watermark is part of the content, not an out-of-band channel, and survives conversion between the analog and digital domains as well as digital and analog format conversions.

A Broadcast Watermark that plugs the Analog Hole exists today. This watermark technology has been extensively tested by DVD CPTWG for DVD video, including passing robustness and Golden Eye testing.

In conclusion, a Broadcast Watermark can provide the protection necessary to prevent unauthorized redistribution of broadcast content and help expand consumer usage and benefits from digital content and distribution.